Transcript of Opening Remarks delivered by Mrs Josephine Teo, Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity at UN's Signature Panel "Building Cyber Resilience for Sustainable Development by Bridging the Global Capacity Gap" (10 May 2024)

Your Excellencies

Chef de Cabinet of the President of the 78th General Assembly Ambassador Kelapile

Secretary General of the ITU, Ms Doreen Bogdan-Martin

Administrator of the UNDP, Mr Achim Steiner

Colleagues and friends

1. Good morning, and I am honoured to address you at today's UN Global Roundtable on ICT Security Capacity Building. The world is more reliant on digital and cyberspace than ever before. In the face of the fast-evolving cyber threats, it is timely that we gathered to discuss the important issue of cyber capacity building. Doreen in her earlier intervention had very eloquently and energetically reminded us of the challenges ahead. In addition to what she has said, and also what Achim and Ambassador Kelapile have contributed, I have three further points to add.

Capacity Building Empowers States by Strengthening and Enhancing State Sovereignty.

2. First, we should think of capacity building as a means to empower States, because they strengthen our abilities to secure our cyberspace and therefore is a way to safeguard our State sovereignty. Capacity building equips States with the skills to protect key national interests, be it their critical information infrastructures like central banks and water supplies, or the protection of our citizens from the modern threat of cybercrime and online scams. By securing the cyber domain, States enhance their own sovereignty while simultaneously uplifting the regional cybersecurity posture.

Empowered States Strengthen the Rules-Based Multilateral Order

3. Second, when States are secure, we are in a better position to strengthen and uphold the rules-based multilateral order, including in cyberspace. For small states such as Singapore, a rules-based international order is critical for our survival as it avoids the situation where might is right. Capacity building enable States, as responsible members of the international community, to perform our international obligations. This includes developing an understanding of how existing international law applies in cyberspace so that we can take actions to uphold it, as well as call out actions that undermine the rules-based order.

Cybersecurity as an Economic Enabler

4. Thirdly, I would add that while many view cybersecurity solely through the national security lens, certainly in ASEAN, we recognise cybersecurity as a critical enabler of the digital economy. It is something that we cannot dispense with. Despite our diversity across languages, political systems, and cultural backgrounds, I'm happy to say that ASEAN Member States collectively recognise the need for a secure cyberspace for the region, so that our citizens and businesses can reap the benefits of a digital economy. Each ASEAN member wants our own citizens to benefit from new technologies to the fullest extent. However, we can only do so if we can mitigate the risks through effective cybersecurity.

5. Vulnerable groups, for example those pointed out by Doreen and Achim – the women, seniors and I would add, Small and Medium Enterprises to the list – they will certainly need our enhanced protection. One key observation is that with increased connectivity, the attack surface is growing exponentially too. And the vulnerable groups are even more exposed than they were ever before. So, it behoves us as States to build cyber resilience in order that we can harness the full potential of digital technologies to uplift our economies. And that is why cyber capacity building is essential. If our citizens cannot connect, transact, and communicate securely on the digital domain, we will be unable to fully capitalise on the benefits.

6. This is also why Singapore is committed to raising our regional cybersecurity posture through capacity building efforts at the ASEAN-Singapore Cybersecurity Centre of Excellence or the ASCCE. Since 2016, we have conducted more than 50 programmes for over 1600 senior officials from the ASEAN Member States. We will continue to do the work through ASCCE. However, while our efforts through the ASCCE are modest, our hope is to offer a concrete way forward to support and uplift our region so that we can collectively gain from digitalisation.

A Need to Groom a Generation of Cyber Leaders for Sustainable Development

7. As I wrap my remarks, I would like to offer three practical suggestions.

8. The first would be for countries to cooperate on cyber capacity building internationally. Singapore looks forward to more partners working with us through the ASCCE and its programmes.

9. Second, cyber capacity building should take a multidisciplinary and multi-stakeholder approach. This is because cybersecurity is a cross-cutting domain. Beyond the operational and technical knowhow, diverse expertise across the policy, legal and diplomatic domains is also required to effectively understand and manage cybersecurity at the national level.

10. My third suggestion would be for States to invest in the next generation of leaders in the cyber domain, even as we cultivate and nurture the current generation. Cybersecurity leadership goes beyond the technical aspects, as it necessitates a broad understanding of the geopolitical, social, and economic implications of cyber threats and cyber operations. In the face of the fast-changing cyber threat landscape, we need leaders who can guide their agencies and ministries through the complexities and technicalities of the domain.

11. There is currently a gap in capacity building efforts to support the development of cyber leaders. Besides the UN-Singapore Cyber Fellowship that we co-organise with the UN Office for Disarmament Affairs, Singapore is committed to address the need through the Singapore Cyber Leadership and Alumni Programme. This programme will take a holistic approach to prepare national cyber leaders in the cross-cutting domains of cybersecurity. The programme will be extended to all UN Member States, including PR Mission representatives in New York and Geneva.

12. Dear colleagues, cyber capacity building efforts are key to building our collective resilience in cyberspace to secure our digital way of life for a sustainable future. I look forward to hearing your diverse views and perspectives in today's Global Roundtable on ICT Security Capacity-Building. Thank you very much for your attention.

+++